UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/608,103	06/30/2000	Christopher L. Hamlin	K35A0631	1085

35219 7590 04/05/2006

WESTERN DIGITAL TECHNOLOGIES, INC.
ATTN: SANDRA GENUA
20511 LAKE FOREST DR.
E-118G
LAKE FOREST, CA 92630

EXAMINER	
COLIN, CARL G	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 04/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/608,103	HAMLIN, CHRISTOPHER L.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 January 2006* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *see att* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 1/9/2006, the following claims 1-16 are presented for examination.

2. Applicant's remarks, pages 2-4, filed on 1/9/2006, with respect to the rejection of claims 1-16 have been fully considered, but they are not persuasive. Applicant argues that the state information cannot be considered a secure drive key because a key is not generated based on the state information. Applicant adds that Trieger does not disclose verifying the authenticity of the encrypted message the authenticator responsive to the encrypted message and the client drive key. Examiner respectfully disagrees. In one embodiment, Trieger discloses generating client drive key based on the key received and client drive ID (column 11, lines 30-55 and column 10, line 57 through column 11, line 2); column 12, discloses more detailed explanation referring to state information (information identified by the key) (column 12, lines 10-15) and also discloses generating client drive key based on the key received and the state information or information identified by the key, for instance, the state information stored in data 1 associated with the key is used to generate new key (column 12). Trieger also discloses a key validation process in the server for verifying the authenticity of the encrypted message, the authenticator responsive to the encrypted message and the generated client drive key (see column 10, line 57 through column 11, line 30) see also embodiment in column 12. With respect to Applicant's argument about the Strokes reference, Examiner respectfully disagrees with applicant's interpretation of the Office

action. The Office action clearly shows that the claimed limitation of "key comprising tamper resistant circuitry" is obvious in view of Stokes. In response to Applicant's argument stating authentication is not done by the devices in Burns, Examiner would like to clarify that the portion of the disclosure below relying by applicant is disclosed by Burns to explain an embodiment where the devices are used as repositories of remotely encrypted data where each network storage is an independent entity, Burns discloses that all encryption being done by the clients (the components of the network that request data from the devices) so that data can remain secured while in transit and so that data travel over the network is stored encrypted rather than being encrypted twice at both the components and the devices; but the storage devices serve as authenticated repository data (column 5, lines 45-59 and column 3, lines 52-60). However, Burns discloses (column 3, line 65 through column 4, line 7) "the network storage devices can be comprised of existing direct-access disk devices and files can be copied directly from one storage device to another in a secure manner, the network clients only involvement would be to initiate the action". Column 7, lines 55-58 recites "request to a network storage device need to be authenticated and guaranteed for freshness, the storage device also enforces access rights"; and column 8, lines 50-52 recites "storage devices guarantee freshness of a request by validating that its own nonce is included in each request hashed message authentication code". The Office action clearly shows that the limitation of receiving internal drive key for use in generating message authentication code and outputting reply data comprising message authentication code is disclosed by Burns. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA

1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In view of the above, applicant has not overcome the prior art and the claims remain rejected in view of the cited prior art.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.1 **Claims 1-16** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,226,750 to **Trieger** in view of US Patent 6,473,861 to **Stokes** and in view of US Patent 5,931,947 to **Burns et al**.

3.2 **As per claims 1, 4-9, and 12-16, Trieger** substantially teaches a secure disk drive comprising: a disk for storing data (see column 6, lines 5-30); (b) and further discloses a message input for receiving the encrypted message from the client disk drive and a data output for outputting the ciphertext data to be written to server's data storage area (see figure 5 and column

11, lines 44-67), the encrypted message comprising ciphertext data and a device ID identifying the client disk drive (see column 10, lines 43-63; column 7, lines 48-55); messages are preferably encrypted (column 9, lines 55-63); and discloses a generator for generating client drive keys based on client drive ID and state information (secure drive key) sent by the client for use to authenticate the client drive ID (column 11, lines 30-55 and column 10, line 57 through column 11, line 2). **Trieger** also discloses a key validation process in the server for verifying the authenticity of the encrypted message and generating an enable signal, the authenticator responsive to the encrypted message and the client drive key (see column 10, line 57 through column 11, line 30); a reply output for outputting reply data and a new key that meets the recitation of internal drive ID (column 11, lines 43-46). Although **Trieger** discloses a secure drive that authenticates a client drive when receiving encrypted request message and output a reply comprising a reply data and a key, **Trieger** does not explicitly disclose a secure drive key comprising tamper resistant circuit and internal drive ID. **Stokes** in an analogous art discloses a secure disk drive comprising: a disk for storing data, secure drive key and internal drive ID, and internal drive keys (see abstract and column 7, lines 16-25); tamper resistant circuitry for storing keys so that any attempt to open the disk drive will result in an erasure of stored encryption key material (column 4, lines 12-25 and column 7, line 50 through column 8, line 18; and see also column 8, lines 48-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention as combined above to modify the secure disk drive of **Trieger** to provide a tamper resistant circuitry for storing keys and to provide secure drive key and internal drive ID for use to authenticate user access (improper user access may lock up the disk drive) as taught by **Stokes**. This modification would have been obvious because one skilled in the art

would have been motivated to do so to provide a drive housing that contains optical and magnetic drives, data encryption and formatted modules and erasable memory device with protective mechanism that automatically erases keys in the event of tampering (see column 3, lines 1-20) and adds additional layer of protecting access by validating user ID or key based on drive keys or internal keys (see column 8, lines 13-67) as suggested by **Stokes**.

Trieger does not explicitly disclose reply data comprising message authentication code. **Burns et al** in an analogous art discloses a data processor comprising: a key input for receiving an internal drive key (see column 8, lines 10-55), internal drive key for use in generating message authentication code (column 9, lines 1-18). **Burns et al** further discloses different protocols in authenticating a response including generating internal drive key based on internal drive ID and secure drive key, for example (see column 8, lines 10-55 and column 9, line 37 through column 10, line 25) and after the request is validated, outputting reply data comprising message authentication code (column 9, lines 14-18) the reply may also contain internal drive ID (column 10, lines 21-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention as combined above to modify the authentication steps of **Trieger** to provide a validation system where all data requests from clients and responses to them are authenticated using keys derived from secure drive keys and hashed message authentication codes as taught by **Burns et al**. The motivation to do so is given by **Burns et al** who teaches that the advantage of this process guarantees freshness preventing replay because nonces are used in the HMAC therefore other entities cannot impersonate either of the devices (column 7, line 55 through column 8, line 4 and column 8, lines 40-53).

As per claims 2 and 10, Stokes discloses the limitation of using a secure drive key that is immutable (see column 4, lines 13-15). Therefore these claims are rejected on the same rationale as the rejection of claim 1.

As per claims 3 and 11, the combined references above discloses generating new key that is mutable in order to invalidate previously issued external client keys (see **Trieger,** column 11, lines 8-20; see **Burns et al**, column 14, line 34-42). Therefore, these claims are rejected on the same rationale as the rejection of claim 1.

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

4.1 The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The prior art discloses generating message authentication using key information and identifier and further discloses key generation based on identifier and keys.

- William Stallings, "Cryptography and Network Security, Principles and Practice", Second Edition, Prentice Hall, Inc. ISBN 0-13-869017-0, pp. 323-353, July 1998.
- Menezes et al., "Handbook of Applied Cryptography", 1997, CRC Press, pg. 171, 357-358.
- Menezes et al., "Handbook of Applied Cryptography", 1997, CRC Press, pp. 500-501.

4.2 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin
Patent Examiner
March 24, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER
cc 3/26/06